



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,703	11/04/2003	Kimitaka Murashita	122.1569	5895
21171	7590	02/23/2009	EXAMINER	
STAAS & HALSEY LLP			JACKSON, JENISE E	
SUITE 700			ART UNIT	PAPER NUMBER
1201 NEW YORK AVENUE, N.W.				
WASHINGTON, DC 20005			2439	
MAIL DATE		DELIVERY MODE		
02/23/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/699,703	Applicant(s) MURASHITA ET AL.
	Examiner JENISE E. JACKSON	Art Unit 2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED. (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 10 November 2008.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 6-11,14-22,27 and 28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) 27-28 is/are allowed.
- 6) Claim(s) 6-11 and 14-22 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/06)
 Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date _____
- 5) Notice of Informal Patent Application
 6) Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 6-11, 14-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ortiz et al(2003/0163710) in view of Ebara(2002/0010862).

3. As per claim 6, Ortiz et al discloses a terminal device includes a biometric data storing unit which stores a plurality of kinds of biometric data associated with a person[0061, 0100, fig. 8 sheet 8]; the plurality of kinds of biometric data including first biometric data used for comparison with biometric data acquired from the person[0027, 0074, 0086], and second biometric data used for comparison with dictionary data; a biometric data acquisition unit which acquires one kind of biometric data from said person[0086, 0096]; a person authentication unit which authenticates said person based on said acquired one kind of biometric data and the corresponding first biometric data among said plurality of kinds of biometric data stored in said biometric data storing unit[0114]. Ortiz discloses biometric data output unit which selects the second biometric data having a different kind than said acquired one kind of biometric data from the plurality of kinds of biometric data of said person[0101-0102]. Ortiz is silent on designated by an authentication device including a dictionary data storing unit storing dictionary data, and outputs the second data from said biometric data storing unit to the authentication device, to authenticate said person by matching said second biometric data with said dictionary data after

said person has been authenticated by said person authentication unit. Ebara discloses from said biometric data storing unit to an authentication device including a dictionary data storing unit storing dictionary data, to authenticate the person by matching the another kind of biometric data with the dictionary data after the person has been authenticated by said person authentication unit[0025-0026, 0028-0029, 0038]. It would have been obvious to one of ordinary skill in the art at the time of the invention to include from said biometric data storing unit to an authentication device including a dictionary data storing unit storing dictionary data, to authenticate the person by matching the output designated biometric data with the dictionary data after the person has been authenticated by said person authentication unit of Ebara with Ortiz, the motivation is that authentication data of Ortiz that has multiple different biometric attributes that can be used to authenticate a user and Ebara's two authentication apparatus can provide flexibility in that a person can be authenticated using two different biometric attributes[0042 of Ebara].

4. As per claim 7, Ortiz et al discloses a biometric data processing unit which edits and processes at least partially said second biometric data selected from said biometric data storing unit, wherein said edited and processed second biometric data is output[0123].

5. As per claim 8, Ortiz discloses a biometric data converting unit which converts the format of said second biometric data selected from said biometric data storing unit, wherein said format-converted second biometric data is output[0032, 0078-0080].

6. As per claim 9, Ortiz discloses a corresponding data generating unit which, from said second biometric data selected from said biometric data storing unit, generates corresponding data having a certain bit length and corresponding to said second biometric data, wherein said generated corresponding data is output from said second biometric data output unit[0087-0089].

7. As per claim 10, Ortiz discloses a corresponding data parameter generating unit which generates a parameter to be used for generating said corresponding data[0073, 0088].

8. As per claim 11, Ortiz et al discloses a terminal device[0023] having a biometric data storing unit which stores a plurality of kinds of biometric data associated with a person[0031-0032, 0034], a biometric data acquiring unit which acquires one kind of biometric data, a second person authentication unit which performs person authentication by matching the one kind of biometric data acquired by the biometric data acquiring unit with the plurality of kinds of biometric data stored in the biometric data storing unit[0023, 0105, 0114]. Ebara discloses and a biometric data transmitting unit which outputs at least another kind of biometric data when the person has been authenticated by the second person authentication unit[0028-0029] and an authentication device having a dictionary data storing unit which stores biometric data as dictionary data to be used for authentication[0038], and a first person authentication unit which performs first person authentication based on said at least another kind of biometric data transmitted from said biometric data transmitting unit and said dictionary data stored in said dictionary data storing unit[0025-0026]. It would have been obvious to one of ordinary skill in the art at the time of the invention to include biometric data output unit which selects and outputs a designated kind of biometric data of the person from said biometric data storing unit to an authentication device including a dictionary data storing unit storing dictionary data, to authenticate the person by matching the output designated biometric data with the dictionary data after the person has been authenticated by said person authentication unit of Ebara with Ortiz, the motivation is that authentication data of Ortiz that has multiple different biometric attributes that can be used to authenticate a user and Ebara's two authentication apparatus can provide

flexibility in that a person can be authenticated using two different biometric attributes[0042 of Ebara].

9. As per claim 14, Ortiz discloses wherein said authentication device comprises a corresponding data generating unit which, based on said biometric data transmitted from said biometric data transmitting unit, generates corresponding data having a certain bit length and corresponding to said biometric data, wherein specific dictionary data stored in said dictionary data storing unit is located by using said generated corresponding data, and said first person authentication unit performs said person authentication based on said specific dictionary data and said transmitted biometric data[0087-0089].

10. As per claim 15, Ortiz discloses wherein when said first person authentication based on said specific dictionary data cannot be performed, said first authentication device performs said first person authentication based on all of said dictionary data stored in said dictionary data storing unit and said transmitted second biometric data[0086, 0124].

11. As per claim 16, Ortiz discloses wherein said terminal device includes a first biometric data processing unit which edits and processes at least partially said second biometric data selected from said biometric data storing unit[0123], and a first processing data storing unit which stores data that said first biometric data processing unit uses to edit and process said second biometric data[0123], and said authentication device includes a second biometric data processing unit which edits and processes said dictionary data at least partially[0105, 0123], and a second processing data storing unit which stores data that said second biometric data processing unit uses to edit and process said dictionary data, and wherein said first person authentication unit performs said person authentication based on said edited and processed

biometric data and said edited and processed dictionary data[0105].

12. As per claim 17, Ortiz discloses wherein said authentication device comprises a conversion data storing unit which stores conversion data concerning said biometric data used in said first person authentication unit, and said terminal device comprises a second biometric data converting unit which converts the format of said second biometric data stored in said second biometric data storing unit, and wherein said biometric data converting unit converts the format of said biometric data by using said format data transmitted from said conversion data storing unit, and said format-converted second biometric data is transmitted to said authentication device[0078-0080, 0083].

13. As per claim 18, Ortiz discloses a first corresponding data generating unit which generates first corresponding data having a certain bit length and corresponding to specific second biometric data selected from along said plurality of biometric data stored in said biometric data storing unit, and a corresponding data transmitting unit which transmits out said generated first corresponding data; the authentication device [0122, 0124], a second corresponding data generating unit which generates corresponding data having a certain bit length and corresponding to said dictionary data wherein, the first person authentication unit which performs first person authentication based on said transmitted first corresponding data and said second corresponding data[0087-0089].

14. As per claim 19, Ortiz discloses wherein said terminal device includes a biometric data acquisition unit which acquires biometric data and a second person authentication unit which performs second person authentication[0023, 0105, 0114], and wherein said second person authentication is performed using said acquired biometric data and said biometric data stored in

Art Unit: 2439

said biometric data storing unit and, when the identity of said person has been authenticated, said first corresponding data to be used in said first person authentication unit is transmitted to said authentication device[0105, 0135].

15. As per claim 20, Ortiz discloses wherein said terminal device includes a first corresponding data parameter generating unit which generates a corresponding data parameter to be used for generating said corresponding data, and wherein said generated corresponding data parameter is not only used in said first corresponding data generating unit, but also transmitted to said authentication device and used in said second corresponding data generating unit[0073, 0088].

16. As per claim 21, Ortiz discloses wherein said authentication device includes a second corresponding data parameter generating unit which generates a corresponding data parameter to be used for generating said corresponding data, and wherein said generated corresponding data parameter is not only used in said second corresponding data generating unit, but also transmitted to said terminal device and used in said first corresponding data generating unit[0073, 0135].

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

- (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

18. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Ortiz(2003/0163710) in view of Ebara and further in view of Uchida(2001/0025342).

19. As per claim 22, Ortiz nor Ebara disclose wherein said authentication device encrypts data that said person has by using said corresponding data used for the authentication of said person as an encryption key. Uchida discloses wherein the authentication device encrypts data that the person has by using the corresponding data used for authentication of the person as an encryption key[0022, 0028]. It would have been obvious of one of ordinary skill in the art at the time of the invention to include biometric data is encrypted biometric data of Uchida with Ortiz, because encrypting biometric data is a protective measure that can enhance security, because even if an unauthorized person steals the biometric data in transit, because the biometric data is encoded[0067 of Uchida] it is intelligible.

Allowable Subject Matter

20. Claims 27-28 are allowable for the following features, “the decryption key is used by the authentication device, the biometric data acquisition device charges a fee to the authentication device for the use”, and “charging a fee to the authentication device according to the number of times that the biometric data stored into the terminal device by the biometric data acquisition device is used by the authentication device”. Prior art of record fails to disclose charging a fee for a decryption key, and charging a fee according to the number of times that the biometric data is stored. In prior art, if a user is enrolled in the system, a user is given a decryption key, there is no suggestion or disclosure of a charge to use a decryption key, and no suggestion in prior art as to how many times biometric data is stored. The Applicant is urged to incorporate allowable

subject matter as stated in claims 27-28, in independent claims 6 and 11. The Applicant contacted Attorney of record, to do an Examiner's Amendment to incorporate claims 27-28 into independent claims 6, and 11. In order to reduce prosecution, the Applicant is urged to amend claims 6 and 11, by incorporating claim limitations of claims 27-28 into claims 6 and 11, or by canceling claims 6 and 11, since claims 27-28 are allowable.

Response to Amendment

21. The Applicant states that Ortiz discloses the second authentication data is acquired, and does not disclose it is selected. The Examiner disagrees with the Applicant. Ortiz discloses [0101] input of a biometric attribute by a user to interface can be based on the random selection of a biometric attribute from a user profile. The number of biometric attributes requested from a user can also be based on a random number. For example, during one authentication session, a user can be requested to provide a left index fingerprint and a left iris scan. During another authentication session, the same user can be required to provide a left index fingerprint, followed by the fingerprint of his or her right middle finger, and immediately thereafter, an iris scan of a left eye, or perhaps, a right eye[0101]. Ortiz also discloses the selection of biometric attributes from the user profile can thus be based on a random selection. The number of required biometric samples that a user can be required to input can also be a random number. Thus, a user can be required to input only three biometric attributes during one authentication session, two biometric attributes during another authentication session, and five biometric attributes during another biometric session[0102].

22. The Applicant states that Ortiz nor Ebara disclose biometric data output unit which

selects and outputs another kind of biometric data of the person, designated by an authentication device. The Examiner disagrees with the Applicant. Ortiz discloses a plurality of biometric attributes can be stored, such as fingerprint and iris data[0100]. Ortiz discloses a system that has a first, second, third biometric attribute input stages. Ortiz discloses during a first biometric attribute input stage; a user can be prompted through a display unit to input his or her name or other word or phrase. During a second biometric attribute input stage, the user can be requested to input his/her right hand. Finally, during a third biometric attribute input stage, the user can be requested to provide a biometric sample of his/her right eye[0105]. Ebara discloses two authentication apparatus; first authentication apparatus acquires the user's biometric information and converts the features to authentication data[0025]. Ebara discloses the second authentication apparatus acquires a user's biometric information, and converts features to authentication. It would have been obvious to include Ebara's two authentication apparatus with Ortiz, because Ortiz has a plurality of biometric data that can be used to authenticate a person, the first authentication apparatus can use one biometric attribute of Ortiz, and the second authentication apparatus can use another biometric attribute [0029 of Ebara and 0105 of Ortiz].

Final Action

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

February 13, 2009
/J. E. J./
Examiner, Art Unit 2439

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434